Network and Information Security Management Discussion Forum 3

*1 - **Learning Outcomes***

- *Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools, and techniques to manage and/or solve them.*
- *Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.*
- *Gather and synthesise information from multiple sources (including Internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues.*
- *Articulate the legal, social, ethical, and professional issues faced by information security professionals.*

Discussion topic

Read the website at Data Protection Commission (2020) Case Studies|Data Protection Commission.

- There are several case studies published during years 2014 – 2018 concerning GDPR related issues and breaches. Considering the case study you have chosen and answer the following questions:
- What is the specific aspect of GDPR that your case study addresses?
- How was it resolved?
- If this was your organisation, what steps would you take as an Information Security Manager to mitigate the issue?

My Initial post

This case study refers to the use of CCTV footage in a disciplinary process of a security guard who was required to monitor the CCTV system at night. Irony aside, the complainant's defence stated he was unaware that the company could use CCTV footage in disciplinary meetings and was a breach the employee's personal data 2003 (Data Protection Commission, n.d.). This pre-GDPR complaint came under the Republic of Ireland's Data Protection Acts 1988-2003 (Data Protection Commission, 2017).

The specific GDPR that addresses this case is Article 6(1)(f) which states the following:

'[where] processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data' (www.gdpreu.org, 2020).

The Data Protection Commissioner's view was the company had a legal basis, *legitimate interests,* for using the CCTV footage for disciplinary proceedings as the complainant's actions could cause reputational and financial loss to the company. Furthermore, the business had used the footage in a minimal manner to corroborate other findings, and the employee had read and signed a Certificate of Understanding and Standard Operating Procedures. Therefore, the Commissioner found in favour of the company.

If I was an information Security Manager, I would have implemented two processes. Annual fraud training for all employees including misuse of company assets and inaccurate reporting of time (Halvorson, 2022). Annual reading and signing of updated company policies in line with legal and contractual obligations of both parties such as Safeguarding, GDPR, SOP, Employee Code of Conduct, and Workplace health and safety (www.indeed.com, 2020).

References

Breach Notification Guidance Under The Data Protection Acts 1988-2003 | Data Protection Commission. (n.d.) *Breach Notification Guidance Under The Data Protection Acts 1988-2003 | Data Protection Commission*. Available from: https://www.dataprotection.ie/en/pre-gdpr/breach-notification-guidance-under-data-protection-acts-1988-2003 [Accessed 25 Apr. 2022].

Case Studies | Data Protection Commission. (2017) *Case Studies | Data Protection Commission*. Available from: https://dataprotection.ie/en/pre-gdpr/case-studies#201704 [Accessed 25 Apr. 2022].

Halvorson, C. (2022) *Managing and Preventing Employee Fraud | When I Work*. [online] wheniwork.com. Available from: https://wheniwork.com/blog/managing-and-preventing-employee-fraud [Accessed 25 Apr. 2022].

https://www.indeed.com. (2020). *company policies signed by employee - Search*. Available from: https://www.indeed.com/hire/c/info/company-policies [Accessed 25 Apr. 2022].

www.gdpreu.org. (2020) *GDPR Legitimate Interests - GDPR EU*. Available from: https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/#:~:text=Legitimate%20interests%20is%20most%20appropriate%20as%20a%20lawful [Accessed 25 Apr. 2022].

Response from: Andrijana Klacar

Hi Jonathan,

I also chose a CCTV case study and had a few thoughts on CCTVs. CCTVs in general have been helpful in different situations such as capturing criminal offences, such as burglaries, abductions, robberies, etc (Love, 2021). Although they offer many benefits, they also come with some disadvantages such as high cost, lack of privacy, followed by vulnerabilities, etc (A1 Security Cameras, 2022).

With the GDPR in sight, there are a few steps that have to be followed in order for organisations to have GDPR compliant CCTVs. First step is the transparency of the usage of CCTV and an explanation of using it. Companies should consider using minimal amount of data (should be limited to what is necessary) and limiting access to only those who need it. Before installing a CCTV, organisations need to carry out a data protection impact assessment (DPIA). DPIA has to be reviewed regularly and

carried out again in case of CCTV movement/upgrade/modification. Lastly, employees can request access of their CCTV images, meaning organisations should search for and provide the requested data in a secure and accessible way (Data Privacy Manager, 2021).

What are your thoughts on surveillance systems?

References:

A1 Security Cameras. (2022) Advantages and Disadvantages of Using Security Cameras. Available from: https://www.a1securitycameras.com/blog/advantages-and-disadvantages-of-using-security-cameras/ [Accessed 27 April 2022].

Data Privacy Manager. (2021) 5 Step Guid to Check if Your CCTV is GDPR Compliant. Available from: https://dataprivacymanager.net/five-step-guide-to-gdpr-compliant-cctv-video-surveillance/ [Accessed 27 April 2022].

Love, J. (2021) 17 Crimes That Were Solved Thanks to Surveillance Footage. Available from: https://www.ranker.com/list/crimes-caught-on-surveillance-cameras/jordan-love [Accessed 27 April 2022].

Response From me:

Hi Andrijana,

Thanks for your reply.

I think with technology usage comes great responsibility.

The Data Protection Act 2018 lists six principles which much be followed by Data Controllers. The Act also mentions subject data rights and location of equipment. (CCTV Information, 2020).

1. Personal data processed lawfully and fairly, if at all.
2. Personal data obtained for specific and lawful purposes.
3. Personal data is adequate and relevant for processing purposes.
4. Personal data is accurate and up to date.
5. Personal data is kept as long as it is needed.
6. Personal data is processed with data subject under this Act.

As well as these principles, the initial assessment should include the following:

1. Reasons and appropriacy of equipment.
2. Persons responsible for the project.
3. Purpose of the scheme.

4. Document standards 1-3.
5. Communicate with Office of the Information Commissioner regarding purpose of use.
6. Person responsible for monitoring scheme compliance.
7. Policies are made available.

Usually when entering a premise in the UK, there is signage notifying people of the use of the CCTV. Do you think people are aware of their rights, or is it a case of ignorance is bliss?

References

CCTV Information. (2020) *The Data Protection Act and CCTV*. Available from: https://www.cctv-information.co.uk/article/the-data-protection-act-and-cctv/.

Initial post from Andrijana:

This post is based on the case study 'Compliance with a Subject Access Request & Disclosure of personal data/capture of images using CCTV' (Data Protection Commission, 2017). A service engineer of a company accused a third-party company of disclosing their personal data (audio recording, CCTV footage) to the engineer's employer without their knowledge/consent. The CCTV footage captured the complainant threatening to "bring down" the third-party company.

The specific case study addresses the GDPR's Chapter 2 Article 5(1)(b) stating the following:

"Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes …" (GDPR, 2016).

The commissioner reviewing the case has concluded that the third-party company had contravened the following Data Protection Acts 1988 and 2003 (2008) Sections (equivalent to the GDPR):

1. 2A (1): "Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the Act of 2003) is complied with by the data controller and at least one of the following conditions is met: …".
2. 2D (1): "… Personal data shall not be treated, for the purposes of section 2(1) (a) …".
3. 2(1) (c)(ii): "the data shall not be further processed in a manner incompatible with that purpose or those purposes".

(Data Protection Commissioner, 2008)

For section 2A (1), the third-party company is accused of its breach as the consent of the complainant was not given. Section 2D (1) was contravened due to the company's lack of transparency, and finally section 2(1) (c)(ii) was contravened due to further processing the engineer's personal data for a reason which was not compatible with the actual purpose for its collection.

To mitigate a similar issue as this case, it is crucial for companies to have zero-tolerance policy towards threats by employees (Dimoff 2018), while also having annually training on companies' policies (SHRM, 2022). Companies should check contract terms and policies with third parties for sharing personal data (CIPD, 2021) and ensure that both companies' and third-party companies' purposes of further processing data comply with GDPR before proceeding (security, 2021).

References:

Data Protection Commissioner. (2008) Data Protection Acts 1988 and 2003: Informal Consolidation. Available from: https://rm.coe.int/16806af232 [Accessed 27 April 2022].

Data Protection Commission. (2017) Case Studies. Available from: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201707 [Accessed 26 April 2022].

GDPR. (2016) Regulations. *Official Journal of the European Union.* N.D.(N.D.): 35.

CIPD. (2021) Data protection and GDPR in the workplace. Available from: https://www.cipd.co.uk/knowledge/fundamentals/emp-law/data-protection/factsheet [Accessed 27 April 2022].

Securiti. (2021) The HR Guide to Employee Data Protection. Available from: https://securiti.ai/blog/hr-employee-data-protection/ [Accessed 27 April 2022].

Dimoff, T. (2018) How to Effectively Deal with Workplace Threats or Violent Behavior. Available from: https://www.cose.org/en/Mind-Your-Business/HR/How-to-Effectively-Deal-with-Workplace-Threats-or-Violent-Behavior [Accessed 27 April 2022].

SHRM. (2022) Understanding Workplace Violence Prevention and Response. Available from: https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplace-violence-prevention-and-response.aspx [Accessed 27 April 2022].

Second response from me:

Hi Andrijana,

Your case study is similar to my case study regarding CCTV footage whereas mine was dismissed, yours was upheld.

It was interesting to read your recommendations, and I would like to add audits. According to (EU GDPR Institute, 2019) a GDPR audit should implemented to determine if the organisation has adequate policies and procedures of personal data. Furthermore, there are two main types of audits: GDPR compliance and Data.

The Data audit is an informal process to help support the formal GDPR compliance audit which examines the following (The SSL Store, 2018):

- What data are we collecting?
- Where are we storing the data?
- How do we protect and document the data?
- How long do we keep the data?
- Do we have a function for every piece of data?
- What is the process for honouring a request to delete data?

These can be done in-house or by a third-party compliance auditor and on a regular basis.

What are your views on this?

Reference list

EU GDPR Institute. (2019) *GDPR Audit Approach*. Available from: https://www.eugdpr.institute/gdpr-audit-approach/ [Accessed 6 May 2022].

The SSL Store. (2018) *GDPR: How to Perform a Data Audit*. Available from: https://www.thesslstore.com/blog/gdpr-data-audit/ [Accessed 6 May 2022].

Response from Andrijana:

Hi Jonathan,

thank you for your informative reply!

Although GDPR audits are not considered to be mandatory, i.e., there is no explicit legal obligation to carry one out, it is good practice for businesses. With the documentation of a GDPR audit, a company can provide these documents to supervisory authorities to prove that it is GDPR compliant. These audits can also reveal internal errors and deficiencies of the GDPR implementations. In this case, companies need to find ways to adapt in order to have full compliance ensured (Wessing, 2020).

I agree with your suggestion about audits. Companies who wish to continue their business legally should carry out audits for their own benefits, internally or externally, in order to keep GDPR requirements satisfied.

References:

Wessing, T. (2020) Compliant or non-compliant? GDPR audits as a self-control tool. Available from: https://www.lexology.com/library/detail.aspx?g=15a03b4c-5657-4be5-8872-4368812e6fc0 [Accessed 10 May 2022].

My summary

This case study refers to the use of CCTV footage in a disciplinary process of a security guard who was required to monitor the CCTV system at night. The complainant's defence stated he was unaware that the company could use CCTV footage in disciplinary meetings and was a breach the employee's personal data 2003 (Data Protection Commission, n.d.). The Data Protection Commissioner's view was the company had a legal basis, *legitimate interests,* for using the CCTV footage for disciplinary proceedings as the complainant's actions could cause reputational and financial loss to the company. *Legitimate interests* falls under the Article 6(1)(f) of the GDPR.

Klacar (2022) mentioned the use of CCTV being helpful in crime reduction; however, the downside to this are privacy issues, infrastructure, and financial costs. Regarding GDPR, companies should implement stages for regulatory compliance purposes. Klacar (2022) recommends the following:

- Be transparent about the use of CCTV.
- Explain reasons for using it.
- Use minimum minimal amount of data/
- Limit access to individuals who require it.
- Access to CCTV footage for employees.
- Do a Data Protection Impact Assessment.

Ashmore (2022) states that a GPDR and a Data audit should be implemented to determine if the organisation has adequate policies and procedures for personal data. The GDPR compliance audit examines the following:

- What data are we collecting?
- Where are we storing the data?
- How do we protect and document the data?
- How long do we keep the data?
- Do we have a function for every piece of data?
- What is the process for honouring a request to delete data?

CCTV is a great way to bolster the security of an organisation; nevertheless, there are regulatory frameworks that ensure organisations handle the individual's data and relevant processes in a reasonable, proportionate, and safe manner.

References

Ashmore, J. (2022) Peer Response. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=305930 [Accessed 10 May 2022].

Case Studies | Data Protection Commission. (2017) *Case Studies | Data Protection Commission*. Available from: https://dataprotection.ie/en/pre-gdpr/case-studies#201704 [Accessed 25 Apr. 2022]

CCTV Information. (2020) *The Data Protection Act and CCTV*. Available from: https://www.cctv-information.co.uk/article/the-data-protection-act-and-cctv/.

Klacar, A. (2022) Peer Response. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=305610 [Accessed 15 May 2022].